Claims

What is claimed is:

1. A system for the verification of an identity of a user, comprising:

(a) an enrollment system comprising:

(i) at least one alphanumeric input device;

(ii) at least one biometric input device;

(iii) at least one header file database having a plurality of identities;

(iv) at least one search engine, said search engine in communication with said header file database such that said search engine receives an alphanumeric data signal which has been input into said alphanumeric input device by the user, and then searches said database for identities that match the alphanumeric data according to a predetermined first set of criteria;

(v) a processor to score the set of identities matched by said search engine according to a predetermined second set of criteria, said processor capable of determining the acceptability or unacceptability of said user's input alphanumeric data based on said score;

(vi) an identity escrow database which is in communication with said processor and receives from said processor an approved identity data signal based on the acceptability of the score, said escrow database additionally in communication with said biometric input device capable of receiving at least one biometric identity data signal input by the user to said biometric input device, said escrow database further comprising means for coupling the approved identity data signal and the biometric identity data signal to create at least one subfile within the escrow database for each user comprising the approved identity data signal and the biometric data signal; and

(b) a verification system for verifying the identity of said user after the user has enrolled in the enrollment system comprising:

(i) means for processing a second input biometric data signal input by the user to the biometric input device to match the user's preexisting biometric data in said escrow database according to a predetermined third set of criteria; and

(ii) an output device for transmitting to a third party whether a match was located within said escrow database for said user.

2. The system of claim 1 wherein said header file database contains bank account opening data.

3. The system of claim 1 wherein the predetermined second set of criteria is mathematically correlated to the per capita rate of fraud arrests in the United States.

4. The system of claim 1 further comprising means for interfacing with the internet so the user and third parties can conduct e-commerce transactions using the system.

5. The system of claim 1 further comprising means for ensuring that the at least one biometric signal and the second biometric signal meet the appropriate standard of sensitivity for the biometric input device employed by the user.

6. The system of claim 5 wherein said ensuring means comprise communication with a Central Biometric Authority database.

7. The system of claim 1 further comprising means for providing the user with a warranty against identity theft.

8. A system for creating an identity escrow file for a user, comprising:

(a) at least one alphanumeric input device;

(b) at least one biometric input device;

(c) at least one header file database having a plurality of identities;

(d) at least one search engine, said engine in communication with said header file database such that said engine receives an alphanumeric data signal which has been input into said alphanumeric input device by the user, and then searches said database for identities that match the alphanumeric data according to a predetermined first set of criteria;

(e) a processor to score the set of identities matched by said search engine according to a predetermined second set of criteria, said processor capable of determining the acceptability or unacceptability of said user's input alphanumeric data based on said score; and

(f) an identity escrow database which is in communication with said processor and receives from said processor an approved identity data signal based on the acceptability of the score, said escrow database additionally in communication which said biometric input device capable of receiving at least one biometric identity data signal input by the user to said biometric input device, said escrow database further comprising means for coupling the approved identity data signal and the biometric identity data signal to create at least one subfile within the escrow database for each user comprising the approved identity data signal and the biometric data signal.

9. The system of claim 8 further comprising storage means for the user to store other electronic data in said escrow database coupled to said approved identity data signal and the biometric data signal.

10. The system of claim 8 further comprising means for accessing said subfile within the escrow database.

11. The system of claim 9 further comprising means for linking said escrow database to third party providers of information specific to said user to be stored in connection with the approved identity data signal and biometric data signal.

12. The system of claim 10 wherein said third party providers are selected from the group consisting of banks, hospitals, doctors, lawyers, and financial services entities.

13. A method for verifying an identity of a user, comprising:

(a) Obtaining alphanumeric identity data from the user;

(b) Obtaining a first biometric exemplar from the user;

(c) Searching the alphanumeric identity data against data in a header file database for matches according to a predetermined first set of criteria;

(d) Processing the matched data of step (c) to score said data according to a predetermined second set of criteria to determine if the user's submitted identity data is approved to create an approved identity data signal;

(e) Coupling the approved identity data signal to the first biometric exemplar to form a subfile within an escrow database.

(f) Processing a second biometric exemplar to match the user's first biometric exemplar in the escrow database and coupled to said approved identity data signal; and

(g) Outputting an approved signal to a third party upon the match of the first and second biometric exemplars of step (f).

14. A system for the verification of an identity of a user, comprising:

(a) an enrollment system comprising:

(i) at least one alphanumeric input device;

(ii) at least one biometric input device;

(iii) at least one header file database having a plurality of identities;

(iv) at least one search engine, said search engine in communication with said header file database such that said search engine receives an alphanumeric data signal which has been input into said alphanumeric input device by the user, and then searches said database for identities that match the alphanumeric data according to a predetermined first set of criteria;

(v) a processor to score the set of identities matched by said search engine according to a predetermined second set of criteria, said processor capable of determining the acceptability or unacceptability of said user's input alphanumeric data based on said score;

(vi) an identity escrow database which is in communication with said processor and receives from said processor an approved identity data signal based on the acceptability of the score, said escrow database additionally in communication with said biometric input device capable of receiving at least one biometric identity data signal input by the user to said biometric input device, said escrow database further comprising means for coupling the approved identity data signal and the biometric identity data signal to create at least one subfile within the escrow database for each user

comprising the approved identity data signal and the biometric data signal;

(b) a verification system for verifying the identity of said user after the user has enrolled in the enrollment system comprising:

(i)means for processing a second input biometric data signal input by the user to the biometric input device to match the user's preexisting biometric data in said escrow database according to a predetermined third set of criteria; and

(ii)an output device for transmitting to a third party whether a match was located within said escrow database for said user; and

(c) means for activating the escrow database other than the second biometric data signal to send a signal to the output device and then to the third party.

15. The system of claim 14 wherein the means for activating the escrow database is a personal identifier (PIN).

16. The system of claim 15 wherein the PIN is a shared PIN.

17. The system of claim 15 further comprising means for adjusting the criteria of sensitivity necessary for the biometric data signal to activate the escrow database to send an approved signal to the output device for different e-commerce transactions.

18. The system of claim 15 further comprising means for obtaining warranty insurance coverage against identity theft.

19. The system of claim 18 wherein said warranty means is a warranty computer linked to the system via the internet.

20. The system of claim 15 further comprising a plurality of enrollment and verification systems running in parallel.